CLAIMS

1. (Currently Amended) A method for constraining delegation by a client to a server, comprising:

a client obtaining a service credential to access a server from a trusted third party;

authorizing the server to access one or more services on behalf of the client by one of:

causing the service credential to specify that delegation of the service credential from the client to the server is authorized; and

causing the trusted third party to maintain an indication that the delegation of the service credential from the client to the server is authorized;

the client receiving the service credential from the trusted third party;

the client providing the service credential to the server;

the client requesting access to a resource through the server;

the server identifying for the client that the resource is provided by a target service that does not reside on the server ~~to which access is sought on behalf of a client~~;

the ~~causing a~~ server itself requesting ~~operatively coupled to the client to request~~ a new service credential to access the target service on behalf of the client from the ~~a~~ trusted third-party;

the client withholding from the server ~~without providing~~ a client's authentication credentials and capability to use the client's authentication credentials; ~~, wherein~~

the server providing ~~provides~~ the trusted third-party with:

a credential authenticating the server; and ~~,~~

I information about the target service; ~~,~~ and ~~a service credential previously provided by the client to the server allowing the client to access the server; and~~

causing the trusted third-party to provide ~~the server with~~ the new service credential that authorizes the server to access the target service on behalf of the client without participation by the client when one of:

the service credential specifies that delegation of the service credential to access the target service is authorized; and

the trusted third-party maintains an indication that the delegation of the service credential to access the target service is authorized.

2. (Original) The method as recited in Claim 1, wherein the trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

3. (Canceled).

4. (Previously Presented) The method as recited in Claim 1, wherein the new service credential is configured for use by the server and the target service to which access is sought.

5. (Previously Presented) The method as recited in Claim 1, wherein the credential authenticating the server is a ticket that includes a ticket granting ticket associated with the server.

6. (Original) The method as recited in Claim 1, further comprising:
causing the trusted third-party to verify that the client has authorized delegation.

7. (Original) The method as recited in Claim 6, wherein:
the trusted third-party includes a key distribution center (KDC); and
causing the trusted third-party to verify that the client has authorized delegation includes verifying the status of a restriction placed on the ticket originating from the client.

8. (Previously Presented) The method as recited in Claim 1, further comprising:

causing the trusted-third-party to selectively determine if the client is allowed to participate in delegation either based on information selected from a group comprising an identity of the client or a group affiliation associated with the client.

9. (Original) The method as recited in Claim 1, wherein the server is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service to which access is sought.

10. (Previously Presented) The method as recited in Claim 1, wherein:

the trusted third-party includes a key distribution center (KDC);

the KDC provides the client's authentication credentials as a ticket-granting ticket associated with the client to the client; and

the client does not provide the ticket granting ticket to the server.

11. (Previously Presented) The method as recited in Claim 1, wherein:

the trusted third-party includes a key distribution center (KDC); and

the server requests the new service credential in a ticket granting service request message that includes the service ticket provided by the client to the server.

12. (Currently Amended) A method for constraining delegation by a client to a server, comprising:

a trusted third party providing a service credential to a client to access a server with delegation of authority by the client to the server to access one or more services signified by one of:

marking the service credential as forwardable to the one or more services; and

maintaining an indication that the server is authorized to access the one or more services on behalf of the client;

the client providing the service credential to the server;

the client requesting access to a resource through the server;

the server identifying a target service not residing on the server to which access is sought on behalf of a client to obtain the resource; and

~~causing~~ the ~~a~~ server ~~operatively coupled to the client to request~~ requesting a new service credential to access to the target service on behalf of the client from the trusted third-party without involving the client in the requesting of the new service credential ~~providing a client's authentication credentials~~, wherein the server provides the trusted third-party with an authentication credential authenticating the server, information about the target service, and the ~~a~~ service credential previously provided by the client to the server, and wherein the service credential previously provided by the client includes implementation-specific identity information constraining a scope of access delegated to the server; and

when the one or more services to which the delegation of authority by the client to the server includes the target service, causing the trusted third-party to provide the server ~~with a~~ the new service credential that authorizes the server without participation of the client to access the target service within the scope of access specified in the implementation-specific identity information.

13. (Original) The method as recited in Claim 12, wherein the implementation-specific identity information includes information selected from a group comprising privilege attribute certificate (PAC) information, security identifier information, Unix identifier information, Passport identifier information, certificate information.

14. (Original) The method as recited in Claim 13, wherein the PAC information includes compound identity information.

15. (Original) The method as recited in Claim 13, wherein the PAC information includes access control restrictions for use as delegation constraints.

16. (Currently Amended) A computer-readable storage medium storing ~~having~~ computer-executable instructions for performing tasks for constraining delegation by a client to a server, comprising:

in a server, determining a target service to which access is sought on behalf of a client coupled to the server; and

in the server, requesting a new service credential from a trusted third-party to access the target service without participation of the client in processing the new service credential and without providing a client's authentication credentials by providing the trusted third-party with a credential authenticating the server, information about the target service, and a service credential that was previously provided to the client and the requesting server such that issuance of the new service credential authorizes the server to access the service on behalf of the client when one of:

the service credential specifies that the service credential is delegable; and

the trusted third-party maintains an indication that the service credential is delegable.

17. (Original) The computer-readable medium as recited in Claim 16, wherein the trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

18. (Canceled).

19. (Previously Presented) The computer-readable medium as recited in Claim 16, wherein the service credential is configured for use by the server and the target service.

20. (Previously Presented) The computer-readable medium as recited in Claim 16, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.

21. (Canceled).

22. (Currently Amended) The computer-readable medium as recited in Claim 16 ~~Claim 21~~, wherein:

the trusted third-party includes a key distribution center (KDC); and

causing the trusted third-party to verify that the client has authorized delegation includes verifying the status of a forwardable flag value as set by the client.

23. (Original) The computer-readable medium as recited in Claim 16, wherein the server is a front-end server with respect to a back-end server coupled to the front-end server, and wherein the back-end server is configured to provide the target service.

24. (Previously Presented) The computer-readable medium as recited in Claim 16, wherein:

the trusted third-party includes a key distribution center (KDC);

the KDC provides to the client authentication credentials of the client as a ticket-granting ticket associated with the client to the client; and

the client does not provide the ticket granting ticket to the server.

25. (Original) The computer-readable medium as recited in Claim 16, wherein:

the trusted third-party includes a key distribution center (KDC); and

the requesting server requests the new service credential in a ticket granting service request message that includes a service ticket provided by the client to the server.

26. (Currently Amended) A system comprising:

a credential granting mechanism configured to:

receive a request for a new service credential from a server and in response generate the new service credential granted in the name of a client rather than the server if delegation is allowable and without providing a client's authentication credentials and capability to use the authentication credentials, and wherein the request includes:

a credential authenticating the requesting server,

identifying information about a target service to which access is sought on behalf of the client coupled to the server, and

a service credential that was previously granted to the client for use with the server; and

grant the request and provide the new service credential to the server allowing the server to access the target service without participation of the client when the delegation is determined to be allowable by one of:

the service credential presenting a forwardable delegation flag indicating the client has authorized the delegation to the target service as being within a scope delegated by the client; and

the credential granting mechanism maintains an indication that the delegation to the server to access the target service is within the scope delegated by the client.

27. (Original) The system as recited in Claim 26, wherein the credential granting mechanism is provided by a trusted third-party and includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

28. (Canceled).

29. (Previously Presented) The system as recited in Claim 26, wherein the service credential is configured for use by the server and the target service.

30. (Previously Presented) The system as recited in Claim 26, wherein the credential authenticating the server includes a ticket granting ticket associated with the server, and which was previously granted by the credential granting mechanism.

31. (Currently Amended) A system for constraining delegation by a client to a server, comprising:

a server configured, on behalf of a client and without the participation of the client, to:

determine that a request from the client seeks access to a resource provided by a target service;

generate a request for a new service credential in the name of the ~~a~~ client rather than the server from a trusted third-party and to be issued to the server to allowing the server to access the target service without providing authentication credentials of the client and without the participation of the client, the new service credential being associated with a client and a target service, the request comprising:

a credential authenticating the server,

information about the target service, and

a service credential associated with the client and the server wherein the server is allowed to access the target service when one of:

the service credential specifies that the service credential is delegable; and

the trusted third-party maintains an indication that the service credential is delegable.

32. (Original) The system as recited in Claim 31, wherein the trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

33. (Original) The system as recited in Claim 31, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.

34. (Original) The system as recited in Claim 31, wherein the server is a front-end server with respect to the service.

35. (Original) The system as recited in Claim 31, wherein the server requests the new service credential in a ticket granting service request message that includes the service ticket associated with the client and the server.

36. (Withdrawn) A computer-readable medium having stored thereon a data structure, comprising:

a credential authenticating a first server,

information identifying a second server, and

a service credential associated with a client and the first server.

37. (Withdrawn) The computer-readable medium as recited in Claim 36, wherein the credential authenticating the first server includes a ticket-granting-ticket (TGT) and the service credential includes a service ticket.

38. (Currently Amended) A method comprising:

separately authenticating a server and a client;

providing the server with a server ticket granting ticket;

providing the client with a client ticket granting ticket and a service ticket for use with the server;

providing the server with the service ticket;

in response to a request by the server, providing the server with a new service ticket for use by the server in accessing the new service for use with a new service without requiring the server to have access to content of the client ticket granting ticket and without the client participating in the request for the new service ticket when one of:

the service ticket specifies that the service credential is delegable; and

the trusted third-party maintains an indication that the service credential is delegable.

39. (Original) The method as recited in Claim 38, further comprising:

causing the server to request the new service ticket on behalf of the client by forwarding the server ticket granting ticket, information identifying the new service, and the service ticket to a trusted third-party.

40. (Currently Amended) A method for constraining delegation by a client to a server, comprising:

a server identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;

causing the ~~a~~ server that is operatively coupled to the target service and the client to use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication protocol method; and

without participation of the client, causing the server to request from the second authentication method trusted third-party a new service credential for use by the server and the target service, from the second authentication method trusted third-party, wherein the server provides the trusted third-party with the credential authenticating the server, information about the target service, and the service credential to itself.

41. (Original) The method as recited in Claim 40, wherein the second authentication method trusted third-party includes at least one service selected from a group of services comprising a key distribution center (KDC) service, a certificate granting authority service, and a domain controller service.

42. (Canceled).

43. (Previously Presented) The method as recited in Claim 40, wherein the service credential is configured for use by the server and the target service to which access is sought.

44. (Previously Presented) The method as recited in Claim 40, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.

45. (Original) The method as recited in Claim 40, further comprising:

upon receiving a request for the new service credential from the server, causing the second authentication method trusted third-party to verify that the client has authorized delegation.

46. (Original) The method as recited in Claim 40, wherein the server is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service.

47. (Original) The method as recited in Claim 40, wherein the first authentication method is selected from a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

48. (Original) The method as recited in Claim 40, wherein the second authentication method includes a Kerberos authentication protocol.

49. (Currently Amended) A computer-readable storage medium storing ~~having~~ computer-executable instructions for performing tasks for constraining delegation by a client to a server, comprising:

a server identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;

causing the ~~a~~ server that is operatively coupled to the target service and the client to use a credential authenticating the server to request a service ticket to itself from a second authentication method trusted third-party by identifying the client and the first authentication method protocol;

causing the server to request a new service ticket configured for use by the server to access the new service without participation of the client ~~and~~ the identified service, from the second authentication method trusted third-party, wherein the server provides the trusted third-party with the credential authenticating the server to the client, information about the target service, and the service ticket to itself; and

causing the second authentication method trusted third-party to issue the new service ticket allowing the server to directly access the new service when one of:

the service ticket specifies the service ticket is delegable; and

the second authentication method trusted third-party maintains an indication that the service ticket is delegable.

50. (Original) The computer-readable medium as recited in Claim 49, wherein the second authentication method trusted third-party includes a key distribution center (KDC).

51. (Canceled).

52. (Previously Presented) The computer-readable medium as recited in Claim 49, wherein the new service ticket is configured for use by the server and the target service.

53. (Previously Presented) The computer-readable medium as recited in Claim 49, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.

54. (Original) The computer-readable medium as recited in Claim 49, further comprising:

upon receiving a request for the new service ticket from the server, causing the second authentication method trusted third-party to verify that the client has authorized delegation.

55. (Original) The computer-readable medium as recited in Claim 49, wherein the server is a front-end server with respect to a back-end server that is coupled to the front-end server, and wherein the back-end server is configured to provide the target service.

56. (Original) The computer-readable medium as recited in Claim 49, wherein the first authentication method is selected from a group of authentication methods comprising Passport, SSL, NTLM, and Digest.

57. (Original) The computer-readable medium as recited in Claim 49, wherein the second authentication method includes a Kerberos authentication protocol.

58. (Currently Amended) A system for constraining delegation by a client to a server, comprising:

a server configurable to:

identify a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method,

use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication method, and

subsequently request a new service credential, for use by the server independently of the client and the target service, from the second authentication method trusted third-party when one of:

the service credential specifies the service credential is delegable; and

the second authentication method trusted third-party maintains an indication that the service credential is delegable,

wherein the server provides the second authentication method trusted third-party with the credential authenticating the server, information about the target service, and the service credential to itself.

59. (Canceled).

60. (Previously Presented) The system as recited in Claim 58, wherein the new service credential is configured for use by the server and the target service.

61. (Previously Presented) The system as recited in Claim 58, wherein the credential authenticating the server includes a ticket granting ticket associated with the server.